

SECURE SYSTEM FOR ACTIVATING PERSONAL COMPUTER SOFTWARE AT REMOTE LOCATIONS

Patent number: JP6501120T

Publication date: 1994-01-27

Inventor:

Applicant:

Classification:

- International: G06F13/00; G06F15/00; H04L9/00; H04L9/00; H04L9/10; H04L9/12

- european: G06F1/00N7R2; G06F9/445; G06F9/445N; G06F21/00N7P5M

Application number: JP19910501845T 19911106

Priority number(s): US19900610037 19901107; US19910682456 19910409

Also published as:

WO9209160 (A1)
EP0556305 (A1)
US5222134 (A1)
EP0556305 (A4)
EP0556305 (B1)

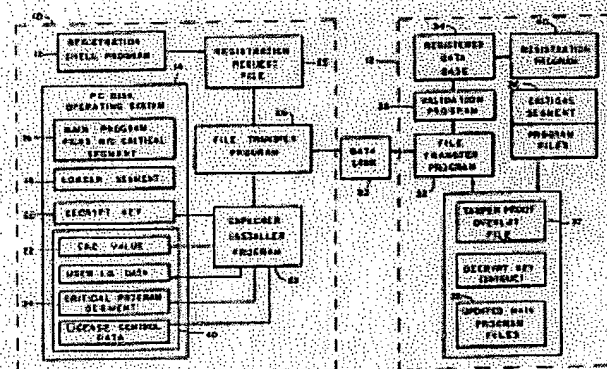
more>>>

Report a data error here

Abstract not available for JP6501120T

Abstract of corresponding document: **US5222134**

A process and system for activating various programs are provided in a personal computer. The computer is initially provided with a registration shell. A data link is established between the personal computer and a registration computer. By providing the registration computer with various information, a potential licensee can register to utilize the program. Once the registration process is complete, a tamperproof overlay program is constructed at the registration computer and transferred to the personal computer. The tamperproof overlay includes critical portions of the main program, without which the main program would not operate and also contains licensee identification and license control data.



Data supplied from the esp@cenet database - Worldwide

BEST AVAILABLE COPY

(19) 日本国特許庁 (J P)

(12) 公表特許公報 (A)

(11) 特許出願公表番号

特表平6-501120

第6部門第3区分

(43) 公表日 平成6年(1994)2月3日

(51) Int.Cl. ³	識別記号	序内整理番号	F I
G 0 6 F 13/00	3 5 1 H	7368-5B	
15/00	3 3 0 A	7459-5L	
H 0 4 L 9/00			
9/10			
	7117-5K	H 0 4 L 9/00	Z
	審査請求 有	予備審査請求 有	(全 8 頁) 最終頁に続く

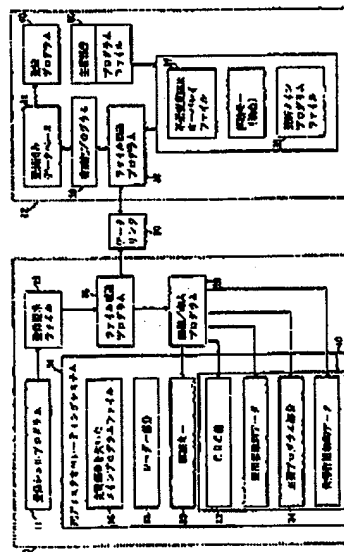
(21) 出願番号 特願平4-501845
 (86) (22) 出願日 平成3年(1991)11月6日
 (85) 翻訳文提出日 平成5年(1993)5月7日
 (86) 国際出願番号 P C T / U S 9 1 / 0 8 0 6 9
 (87) 国際公開番号 W O 9 2 / 0 9 1 6 0
 (87) 国際公開日 平成4年(1992)5月29日
 (31) 優先権主張番号 6 1 0 , 0 3 7
 (32) 優先日 1990年11月7日
 (33) 優先権主張国 米国 (U S)
 (31) 優先権主張番号 6 8 2 , 4 5 6
 (32) 優先日 1991年4月9日
 (33) 優先権主張国 米国 (U S)

(71) 出願人 タウ システム コーポレーション
 アメリカ合衆国 バージニア州 フォルス
 チャーテ, リースバーグ バイク,
 7115, スーツ327
 (72) 発明者 ワイト, デービット, ビー
 アメリカ合衆国 バージニア州 22032,
 フェアファックス ギルバートソン ロード,
 4220
 (72) 発明者 リッデル, ホレイス, ジー
 アメリカ合衆国 バージニア州 22021,
 チャンチレイ, バレイ カウントリ ドラ
 イブ, 13811
 (74) 代理人 弁理士 倉持 裕 (外1名)
 最終頁に続く

(54) 【発明の名称】 パーソナルコンピュータのソフトウェアを遠隔位置で起動するための安全システム

(57) 【要約】

様々なプログラムを起動するための過程とシステムがパーソナルコンピュータ(10)に提供されている。パーソナルコンピュータ(10)には、登録シェルプログラム(11)が当初備わっている。データリンク(20)がパーソナルコンピュータ(10)と登録用コンピュータ(12)の間に確立される。登録用コンピュータ(12)に様々な情報を与えることにより、見込み被許諾者はメインプログラム(16)の使用を登録することができる。ひとたび登録過程が完了すると、不正変更防止オーバーレイプログラムが登録用コンピュータ(12)において作成され、パーソナルコンピュータ(10)に転送される。不正変更防止オーバーレイには、メインプログラム(18)の主要部分がふくまれ、これを欠くとメインプログラム(16)は動作せず、また不正変更防止オーバーレイには使用許諾識別データと使用許諾制御データも含まれている。



【請求の範囲】

1. プログラムファイルを起動する方法であって、
表示装置を有する遠隔コンピュータに対して、ローダープログラムと登録シリアル部分を含むプログラムファイルを提供し、上記プログラムファイルは主要部分を欠いて、上記プログラムファイルを正しく実行することを防止する工程、
使用者識別情報を上記登録シリアル部分に入力する工程、
上記使用者識別情報を、上記登録シリアルから登録用コンピュータ内にある独立した登録プログラムに転送し、上記登録プログラムは使用者識別データと上記主要部分を結合して独自のオーバーレイファイルを作成する工程、
上記の独自のオーバーレイファイルを上記登録プログラムから上記登録シリアルに転送する工程、上記オーバーレイファイルには上記プログラムファイルには記載されていない主要部分が含まれ、そして
上記オーバーレイファイルを上記メインプログラムファイルに導入する工程を有し、上記オーバーレイファイルに入っている使用者識別が導入されたときだけ上記プログラムファイルの動作が可能とすることを特徴とする前記のプログラムファイル起動方法。
2. 上記オーバーレイファイルを上記登録用コンピュータから上記遠隔コンピュータに転送する前に、上記使用者識別情報を利用可能にする工程を有する請求の範囲第1項に記載の方法。
3. 不正変更防止のオーバーレイファイルを作成する工程を有する請求の範囲第1項に記載の方法。
4. 上記不正変更防止オーバーレイファイルが上記オーバーレイファイルを暗号化することにより作成され、巡回冗長検査値が上記

主要プログラム部分が欠けているプログラムファイルが盗用されている、このプログラムファイルが動作することを防止し、上記オーバーレイローダー部分は本物のオーバーレイファイルが現在導入されているときだけこのプログラムファイルを起動することができ、上記登録コンピュータには登録シリアルプログラムが備えられ、上記登録シリアルプログラムは使用者が様々な使用者識別情報を入力することを可能にするような少なくとも一つの遠隔コンピュータと、

登録プログラムと、上記使用者識別情報を受信し処理するための手段と、上記プログラムファイルに欠けている上記主要プログラム部分と使用権限情報情報の全部あるいは一部を含む独自のオーバーレイファイルを作成するための手段と、上記オーバーレイファイルを上記遠隔コンピュータに転送する手段とを備えた登録用コンピュータとを有し、

上記オーバーレイファイルを上記遠隔コンピュータに転送することで、上記オーバーレイファイルに入っている使用者識別が現在導入されているときだけ上記プログラムファイルの動作が可能になることを特徴とする上記プログラムファイル起動システム。

11. 上記遠隔コンピュータと上記登録用コンピュータとの間を結合する電子データリンクと、上記登録用コンピュータと上記遠隔コンピュータの両方に備えられているファイル転送装置とを含むことを特徴とする請求の範囲第10項に記載のプログラムファイル起動システム。

12. 上記登録用コンピュータが、すべての登録済み使用者が含まれている中央データベースと上記使用者識別情報を暗号化するための手段とを備えていることを特徴とする請求の範囲第10項に記載のプログラムファイル起動システム。

特許第6-501120 (2)

暗号化オーバーレイファイル内にあるとともに、暗号キーを上記オーバーレイファイルに格納する請求の範囲第8項に記載の方法。

5. 上記オーバーレイが実行のためにロードされるたびに巡回冗長検査値が計算され、上記不正変更防止オーバーレイファイル内に転送された巡回冗長検査値と比較され、上記オーバーレイファイルが作成以後変更されているかどうかを判断することと特徴とする請求の範囲第4項に記載の方法。

6. 上記使用者識別情報と上記オーバーレイファイルとが、電子データリンクを介して上記登録シリアルと上記登録プログラムとの間を転送されることを特徴とする請求の範囲第1項に記載の方法。

7. 上記登録シリアルプログラムが、上記の独立した登録用コンピュータを備えた第二の遠隔コンピュータから離れた、第一のコンピュータ内に格納されていることを特徴とする請求の範囲第1項に記載の方法。

8. 上記利用可能工程によって上記使用者識別情報が正式の登録シリアルを確保することを特徴とする請求の範囲第2項に記載の方法。

9. 上記使用者識別と上記オーバーレイファイルが、一台のコンピュータに入力され備えられることを特徴とする請求の範囲第1項に記載の方法。

10. プログラムファイルを複製されたもしくは創製されない期間を短縮するためのシステムにおいて、

オーバーレイローダー部分が含まれている少なくとも一つの

13. オーバーレイファイルを作成するための上記手段が、巡回冗長検査値を備える不正変更防止オーバーレイファイルを作成するための暗号化装置と暗号キーを備えており、上記暗号キーは上記オーバーレイファイルと共に上記遠隔コンピュータに転送されることを特徴とする請求の範囲第10項に記載のプログラムファイル起動システム。

14. 上記遠隔コンピュータが、上記オーバーレイファイルを解放し、上記オーバーレイファイルが実行のためにロードされるたびに巡回冗長検査値を計算し、そしてこの検査値を上記登録用コンピュータによって上記オーバーレイファイルと共に転送された巡回冗長検査値と比較するための手段を備えていることを特徴とする請求の範囲第12項に記載のプログラムファイル起動システム。

15. 上記主要部分がエグゼクティブ制御部分であり、そして上記使用者識別情報が使用許諾契約情報であることを特徴とする請求の範囲第1項に記載の方法。

16. 上記主要プログラム部分がエグゼクティブ制御プログラムであり、そして上記使用者識別情報が使用許諾契約情報であることを特徴とする請求の範囲第10項に記載のプログラムファイル起動システム。

17. 上記主要エグゼクティブ制御プログラム部分がプログラムファイル全体を有することを特徴とする請求の範囲第16項に記載のプログラムファイル起動システム。

18. プログラムファイルの使用を制御する方法において、
表示装置を有するコンピュータに対してローダー部分と登録シリアル部分を含むプログラムファイルを提供し、上記プログラムフ

特表平6-501120 (9)

ファイルは第一レベルの制御機能を有するエグゼクティブ制御プログラムを有しており、

情報を上記登録レベル部分に入力し、

上記使用許諾契約情報を上記登録レベルから独立登録プログラムに伝送し、上記登録プログラムは使用許諾契約データを第二レベルの制御機能を有するエグゼクティブ制御プログラムに併合して独自のオーバーレイファイルを生成し、

上記独自のオーバーレイファイルを上記登録プログラムから上記登録レベルに伝送し、上記オーバーレイファイルには上記第二レベルのエグゼクティブ制御プログラムが含まれており、そして

上記独自のオーバーレイファイルを上記登録プログラムファイルに導入し、上記プログラムファイルの第二レベルの機能の動作が上記オーバーレイファイル内の使用許諾契約情報が読み込まれているときだけ可能になることを特徴とする上記のプログラムファイル使用の制御方法。

19. 上記オーバーレイファイルを上記登録用コンピュータから上記登録コンピュータに伝送する以前に、上記使用許諾契約情報を有効化する工程を有する請求の範囲第18項に記載の方法。

20. 不正変更防止になっているオーバーレイファイルを検出する工程を有する請求の範囲第18項に記載の方法。

21. 上記不正変更防止オーバーレイファイルが上記不正変更防止オーバーレイファイルを暗号化キーで暗号化することにより作成され、巡回冗長検査値を上記暗号化不正変更防止オーバーレイファイル内に提供するとともに暗号化キーを上記不正変更防止オーバーレイファイルに提供し、上記暗号化および暗号化キーは上記オーバーレイファイルの独自の内容によって自由に決定されることを特徴とする請求の範囲第20項に記載の方法。

上記登録レベルプログラムは使用者が様々な使用許諾契約情報を入力することを可能にするよう少なくとも一台の登録コンピュータと、

登録プログラムと、上記使用許諾契約情報を受信し処理するための手段と、第二レベルの機能を有するプログラムモジュールと使用許諾契約情報の全量あるいは一部を含む独自のオーバーレイファイルを作成するための手段と、上記オーバーレイファイルを上記登録コンピュータに伝送する手段とを備えた登録用コンピュータとを有し、

上記オーバーレイファイルを上記登録コンピュータに伝送することで、上記オーバーレイファイルに入っている使用許諾契約情報が現在使われているときだけ、上記プログラムファイルの第二レベルの機能の動作が可能になることを特徴とする上記システム。

22. 上記登録コンピュータと上記登録用コンピュータとの間に電子データリンクを有し、ファイル転送機能が上記登録用コンピュータと上記登録コンピュータの両方に備えられていることを特徴とする請求の範囲第21項に記載のシステム。

23. 上記登録用コンピュータが、すべての登録済み使用者が含まれる中央データベースと上記使用許諾契約情報を有効化する手段とを備えていることを特徴とする請求の範囲第22項に記載のシステム。

24. オーバーレイファイルを作成するための上記手段が、巡回冗長検査値が記憶されている不正変更防止オーバーレイファイル作成するための暗号化キーと暗号化キーとを備えており、上記暗号化キーは上記オーバーレイファイルと共に上記登録コンピュータに伝送され、上記暗号化および暗号化キーはファイルの内容によって自由に決定されることを特徴とする請求の範囲第23項に記載のシステム。

22. 新しい巡回冗長検査値が、上記オーバーレイが実行のためにロードされるたびに計算されて、上記オーバーレイファイルと共に伝送された巡回冗長検査値と比較され、上記オーバーレイファイルが作成以降変更されているかどうかを判断することを特徴とする請求の範囲第21項に記載の方法。

23. 上記使用許諾契約情報と上記オーバーレイファイルが、上記登録レベルと上記登録プログラムとの間に電子データリンクを介して伝送されることを特徴とする請求の範囲第18項に記載の方法。

24. 上記登録レベルプログラムが、上記独立登録プログラムを備えた第二のコンピュータから離れている第一のコンピュータに備えられていることを特徴とする請求の範囲第18項に記載の方法。

25. 上記有効化により上記使用許諾契約情報が正次の登録レベルを介して有効であることを特徴とする請求の範囲第19項に記載の方法。

26. 上記使用許諾契約情報と上記オーバーレイファイルが一台のコンピュータに入力され、備えられていることを特徴とする請求の範囲第18項に記載の方法。

27. 記憶されたあるいは記憶されない期間、プログラムファイルがアップグレードするシステムにおいて、

第一レベルの機能の動作を有するプログラムを含むオーバーレイローダーを含むプログラムファイルが記憶されていて、上記オーバーレイローダー部分は本物のオーバーレイファイルが読み込まれているときだけこのプログラムファイルを起動することができ、上記登録コンピュータには登録レベルプログラムが備えられ、

システム。

28. 上記登録コンピュータが、上記オーバーレイファイルを解読し、上記オーバーレイファイルが実行のためのロードされるたびに新しい巡回冗長検査値を計算し、そしてこの検査値を上記登録用コンピュータにより上記オーバーレイファイルと共に伝送された巡回冗長検査値と比較するための手段を備えていることを特徴とする請求の範囲第20項に記載のシステム。

特開平6-501120 (4)

【明 明 書】

パーソナルコンピュータのソフトウェアを盗用位置で起動するための資金システム

発明の概要

一般的に、パーソナルコンピュータあるいはそれに類似した装置の使用の大部分は、それら装置で実行するソフトウェアを様々な形態からあるいは複製販売を通じて入手する。いずれの場合も、ソフトウェア製品はいわゆる「紙箱包装」材で包装されており、その紙箱包装を破った時点でそのソフトウェア製品に対する使用許可契約が成立して、その製品の使用許諾者（被使用許諾者）/購入者による使用可能範囲あるいは使用から保護するようになっている。この方法による商取引は、許諾者と被使用許諾者の双方にとって満足すべきものではないことが分かっている。たとえば、被使用許諾者にとっては、ソフトウェアプログラムを操作させてみてからそれが使用許諾が必要としているものかどうかを判断する機会が与えられない。さらに、許諾者の側からみると、この方法では被使用許諾者の識別ができないという、許諾者によるプログラム使用の制限あるいは監視を行なうことができない。

ソフトウェアプログラム保護方式は、Thomsonの米国特許第4,446,519号に開示されており、プログラムされた「はい/いいえ」で書える装置がプログラムに組み込まれており、そのソフトウェアが使用許可されるコンピュータに設置されているハードウェアあるいはファームウェア保護装置の存在を認識するようになっている。この装置の意図は、プログラムが物理的な複製を複製しては使用できないようにすることであり、これはソフトウェアよりも単純なことがはるかに困難である。しかし、このような方法は、正しい符号化店客が見破られ、そしてそれをわずかに変えてプログラムに書き込まれてしまえば、簡単に打ち破られてしまう。ひとたび打ち破られると、無制限の盗用コピーが作成され配布される可能性がある。

本発明は、パーソナルコンピュータのソフトウェアプログラムあるいは他の種類のプログラムを、使用許可を管理する方法で配布する方法とシステムに関する。動作可能プログラムは、購入者/被許諾者と販売者/許諾者との間の特定の契約において入手可能になる。販売者と購入者との関係は、本発明の目的に照しては、許諾者/被許諾者間の関係である必要はないが、以下では販売者を許諾者、購入者を被許諾者もしくは使用者と称す。ひとたび被許諾者が特定の契約条件に合意すると、被許諾者識別データが被許諾者コンピュータに与えられる。登録用コンピュータはその契約を記憶し、使用許可されたプログラムの可動部分を生成する。これらの部分は不正複製防止が施されていると同時に、盗用された被許諾者にとって独自のものとなっている。この情報の交換に基づき、可動コンピュータプログラムが登録用被許諾者のコンピュータに不正複製防止ファイルに収納されて配布される。同時に、このファイルには被許諾者独自の情報が含まれている。本発明の実施例としては様々なものが考えられるが、いずれの実施例も被許諾者を識別する独自のデータと保護されているソフトウェアプログラムに関する情報とが含まれている符号化パッケージの構造を作っている。したがって、被許諾者は匿名ではなく、そして保護されたソフトウェアは使用許諾契約に違反できる情報で付帯化される。さらに、使用許可制御データは符号化パッケージに含めることにより、様々な複製を防止して使用許可契約の条件を遵守させることができる。

一般的に、様々な実施例は、ソフトウェアのデモンストレーション版を有する可能性のあるマーケティングシミュレーションプログラムの最初の配布が行う。このシミュレーションプログラムは、見本版と直接記述だけを有しているか、あるいは完全なプログラムの動作不能版を有している。しかし、大部分の実施例は、登録プログラムと、ローディングメントと呼ばれる特定のプログラムモジュールを含むような構成になっている。

マーケティングシミュレーションは適切な方法で自由に配布されるであろう。マーケティングシミュレーションがプログラムのデモンストレーション

Williamの米国特許第4,740,890号は、中央（盗用）コンピュータを盗用して、正しい符号の入手を試みる悪意のプログラマーがアクセスできないマスターリストあるいはアルゴリズムから得られたコピー解除コードあるいは有符号コードを提供することを開示している。しかし、この方法は、仮定中のコードを受け受けることにより、あるいは盗用の周囲をプログラミングすることにより、もしくはデバッガープログラムによりプログラムを分析してプログラムの実行を可能にするコードの存在を見つ出すことにより、簡単に克服されてしまう。ひとたびこの保護が打ち破られると、動作可能なプログラムの無制限のコピーが作成され配布される可能性がある。

さらに、Schmidtの米国特許第4,649,510号に開示されている方法では、最も信頼のあるアルゴリズムを無符号化し、無符号化されたプログラムを処理装置内で実行すると同時に、回復アルゴリズムを別の物理的に分離した装置で実行することにより回復し、有効結果を2つの処理装置の相互通信によって獲得するようになっている。このような方法は、回復アルゴリズムの管理の保護に依存しており、この物理的保護が侵害された場合、悪意のプログラムによって簡単に打ち破られる可能性がある。したがって、そのような方法は、回復記憶媒体の物理的保護が提供できない大量市場においては、実用的ではない。

そのため、ソフトウェアを容易に使用から保護しつつソフトウェアを大量市場に配布するための経済的な方法が求められる。さらに、見込み購入者/被許諾者がソフトウェア製品を購入前に試してみることができよう方法とシステムも必要である。また、ソフトウェア製品の改良および更新部分と並進使用に配布するための方法も必要である。

発明の簡単な説明

本発明は、パーソナルコンピュータのソフトウェアプログラムあるいは他の種類のプログラムを、使用許可を管理する方法で配布

版を有している場合、ニグゼクティブ制御ループが保護されたプログラムの固定版になる。マーケティングシミュレーション版は、登録用コンピュータにインストールされる。マーケティングシミュレーション版のプログラムは、登録データと登録データベースコンピュータに記憶する。符号化ファイル内で結合された被許諾者独自のデータと動作可能版のプログラムとを有する独自の符号化パッケージが組み立てられる。独自の符号化パッケージは、符号化ファイルおよび保護されているプログラムファイルと共に被許諾者のコンピュータに伝送されるが、これらはマーケティングシミュレーション版を大きくする。被許諾者、符号化ファイル、そして保護されていないファイルの削除と同時に、マーケティングシミュレーション版はこれらの各々を使用者のコンピュータに導入する。

したがって、被許諾者がプログラムを実行する毎に、ローディングメントが提供された解読キーを使用して、符号化ファイルを保護されていないファイルに対するオーバーレイとしてロードして解読する。このプログラムは保護されていないソフトウェアプログラムの設計にしたがって実行され、独自の使用許諾データもプログラム実行中にロードされる。プログラムが実行されている間は、保護されているプログラムはその符号化形態に留まって、保護されていないプログラムファイルと共にコンピュータの大量記憶装置に格納されている。保護されているプログラムは実行のためにロードされたときだけ解読され、正しい符号化キーにアクセスしなければ変更され得ない。

図面の簡単な説明

図1は本発明による登録過程を示す流れ図である。
図2は本発明によるプログラム実行過程を示す流れ図である。
図3は、本発明の知見による代表的なパーソナルコンピュータと登録用コンピュータの概略図である。
図4は、本発明の知見による代表的なパーソナルコンピュータと登録用コンピュータに代る実施例を示す概略図である。

特表平6-501120(5)

発明の詳細な説明

本発明の目的は、許諾者がそのプログラムの費用対効果に関する責任を従来使用されている方法よりはるかに効率的な方法で維持することを可能にすることである。さらに、本発明の第二の目的は、被許諾者あるいは使用者が特定のプログラムの購入あるいは使用許諾を得る前に試用することを可能にすることである。さらに、本発明の更なる目的は、特定のプログラムの使用許諾保護されたアップグレード版を登録被許諾者に配布する手段を提供することである。したがって、本発明の利点は包括的なものと見られ、そしてどのようなソフトウェアプログラムも本方法によって配布できるものと見なされている。

一実施例において、動作可能なエグゼクティブ制御ループを除いて完全な製品プログラムが、パーソナルコンピュータあるいは他の装置において、磁気ディスク、フロッピーディスク、ハードウェアあるいは他の手段で最初に提供される。さらに、この特定プログラムには登録シミュレーションプログラムも含まれる。ただし、小さいプログラムもしくは短く短いプログラムの場合、プログラム自体は存在せず、シミュレーションだけが提供される。エグゼクティブ制御ループが除外されているため、このプログラムは正しい登録過程を再現しなければ動作しない。図1および図2に示されているように、この登録過程は、パーソナルコンピュータ(PC) 10内部の登録シミュレーションプログラム11と登録用コンピュータ12内部に提供されている登録プログラム40とを使用して開始される。登録システムプログラムが登録用コンピュータ12内に提供され、電子データリンク30を介して登録シミュレーションプログラムがアクセスできる。この電子データリンクは、ローカルエリアネットワークでもよく、電話モデムリンクでもよく、あるいはその他のいかなる媒体であってもよい。ただし、第二の実施例においては、登録シミュレーションシステムプログラムは同一の媒体上に存在してもよいが、その媒体は製品応用プログラムとは別でなければならぬ。この場

合、登録シミュレーションおよび登録システムプログラムが入っている共通可能な媒体は、許諾された導入プログラムによって使用者パーソナルコンピュータ10へ個人的に移送され、電子データリンクは必要ではない。

登録シミュレーションプログラムは、使用者がPCオペレーティングシステム14のメインプログラムファイル内に提供されている製品応用プログラムの実行を最終に許可すると実行される。登録シミュレーション製品応用プログラムに関する記述情報を提供しそれをPC表示装置に表示すると同時に、見込み被許諾者を促進して候補者として登録する。使用許諾は、特定の適用場所における特定の被許諾者に対して提供され、その期間には様々な長さもしくは一時的でよく、そのための費用は被許諾者に対して課せられない。ただし、登録シミュレーションは、不正使用防止オーバーレイファイルが存在しないかぎり、メインプログラムを実行しない。登録シミュレーションプログラム11は、被許諾者のPCに提示されるデータ入力形式を提供し、被許諾者に対して、請求書送付先、口座番号、使用許諾条件などの識別情報の提供を要求する。この情報は、被許諾者が再帰する登録要求ファイル35に入力される。そして、登録シミュレーションプログラムは、被許諾者が指定キーを押して登録を開始するのを待つ。このキーが押されると、登録ファイルが同じ、そして登録シミュレーションプログラム26が登録システムファイル転送プログラムとのデータリンクを確立する。登録用コンピュータ12内の登録プログラム40は、データリンクが正当な登録シミュレーションで確立されていることを確認する秘密保護チェックを実行する有効化手段によって保護される。つまり、登録シミュレーション登録要求ファイル35を、そのファイルを受信する登録システムに転送し、必要ならデータリンクと、結合されたファイル転送プログラム26および32間のハンドシェイク動作を実行する。完全な登録要求ファイルが中央登録用コンピュータで受信されると、登録要求が登録済み使用者34のデータベースに対して格納される。確認には、その要求に答えるべきかど

うかを判断する様々なチェックが含まれる。たとえば、一時的使用許諾に対する要求が特定の被許諾者から再度送られてきた場合、その被許諾者には使用許可が与えられず、そしてそのプログラムのエグゼクティブ制御ループは過期されない。そのような状況が発生した場合、適切なメッセージが登録シミュレーションに転送され、見込み被許諾者に対して表示される。しかし、要求が承認されると、登録済み使用者データベースへの登録が作成されるが、この過程全体が完了するまで、そのデータベースには入力されない。

登録用コンピュータ12の内部では、つまり使用登録データが使用されて、使用登録データとエグゼクティブ制御ループプログラム命令30とを結合することにより作成された独自の不正使用防止オーバーレイファイルが生成される。結合されたデータとプログラムファイルに結合で、不正使用防止オーバーレイファイル31内におかれる巡回冗長検査(CRC)値が計算される。一意の独自の暗号化キーと解読キーが作成され、不正使用防止オーバーレイファイルの内容全体が暗号化キーを使用して暗号化される。この暗号化キーに基づき、不正使用防止オーバーレイファイルと共に提供される解読キーが提供される。暗号化アルゴリズムは、登録暗号化システムのように、暗号化と解読にそれぞれ異なるキーを使用する拡張であればなんでもよい。登録システムが、不正使用防止オーバーレイファイルと解読キーを、パーソナルコンピュータ登録シミュレーションに転送される1個の出力ファイル38に組み込む。また、更新されたメインプログラムファイルもこの出力ファイルに組み込まれ、ファイル転送プログラムとすでに確立されているデータリンクとを介してPCの登録システムに転送される。

出力ファイル一式の受信と同時に、登録シミュレーション内の開通導入プログラム34が出力ファイルを開き、エグゼクティブ制御ループセグメント36、CRC値38ならびに解読キー30および、含まれている場合は、更新メインプログラムファイルを含む不正使用防止オーバーレイファイル40を導入する。これで登録過程が

完了したので、電子データリンクを切断する。登録データベースレコードが入力され、そして被許諾者の要求に対する解決が、中央登録用コンピュータ12における別のプログラムによって実行される。

登録が終了すると、被許諾者のパーソナルコンピュータに導入された従来の製品応用プログラムを起動して、不正使用防止オーバーレイファイルと解読キーを使用して製品応用プログラムを実行するたびに実行する製品応用プログラム一式をロードするためのプロセスが開始される。

このプログラム実行過程を図1に示す。図示されているように、パーソナルコンピュータの使用者が製品応用プログラムの実行をオペレーティングシステムに命令すると、オペレーティングシステムはメインプログラムとローダーセグメントをロードする。ローダーセグメントは他のすべてのプログラム命令に先立って実行される。つまり、ローダーセグメントは製品応用プログラムの起動を実行し、不正使用防止オーバーレイの存在をチェックする。不正使用防止オーバーレイが導入されていないければ、ローダーセグメントは終了してオペレーティングシステムに戻る。メインプログラムファイルの実行が事前に防止される。不正使用防止オーバーレイが導入されているれば、ローダーセグメントは解読キーを用いて不正使用防止オーバーレイの解読とロードを行ない、メインプログラムファイルに対して秘密でないエグゼクティブ制御ループプログラム命令ならびに独自の識別および使用許諾制御データを渡す。解読およびロード過程において巡回冗長検査値が提供され、それが完了すると、不正使用防止オーバーレイが登録済みコンピュータからパーソナルコンピュータに転送されたときに作成された不正使用防止オーバーレイに記憶された巡回冗長検査値と比較される。巡回冗長検査値が失敗に終わると、そのオーバーレイは何らかの方法によって復元が与えられたものとみなされ、したがって無効とされる。この時点で、ローダーセグ

特表平6-501120 (6)

ントはそのオーバーレイを取り外し、終了してオペレーティングシステムに戻る。したがって、不正変更防止オーバーレイが含まれていない場合と同様に、メインプログラムファイルの実行は、不正変更防止オーバーレイのどの部分が変更されていても、事前に防止される。盗用元長検査の結果、オーバーレイが変更されていないことが確認されると、ローダーセグメントはオーバーレイを含むメインプログラムファイルの実行を開始し、そして製品応用プログラムが最後まで実行される。

不正変更防止オーバーレイを動作可能形態の製品応用プログラムに含めることを要求することにより、盗用者識別と使用許諾制御データはそれ以降動作可能プログラムに常に含まれることになる。このようにして、盗用者は不正使用を防止するとともに監視することが出来る。

図1および図2を参照しながら説明したように、本発明によると、登録過程によって、メインプログラムファイルのニグゼクティブ制御ルーブセグメントと使用許諾制御データを含む不正変更防止オーバーレイファイルが作成される。登録過程が完了すると、この不正変更防止オーバーレイは登録用コンピュータからパーソナルコンピュータに転送される。この不正変更防止オーバーレイは、起動時に不正使用を防止するキー装置である。なぜなら、エグゼクティブ制御ルーブプログラム命令は、内容なしに独自の使用許諾制御データと使用許諾制御データから分離することでもできなければ、盗用者識別と使用許諾制御データも内容なしには変更できないからである。

この不正変更防止オーバーレイファイルは、オーバーレイファイルが作成されるときに最初に盗用元長検査をオーバーレイファイルに記憶させると不正変更防止になるとみなされる。盗用元長検査は、プログラム命令と使用許諾データを含むオーバーレイファイルの内容全体に対して計算される。盗用者データは独自であるので、各々のCRCは独自なものになる。記憶されてい

るCRC値が、オーバーレイがロードされるたびにローダーセグメントによって計算された盗用元長検査値と比較される。これらの盗用元長検査値が一致しなければ、ローダーセグメントは終了してオペレーティングシステムに戻る。したがって、オーバーレイファイルの内容にせよならかの変更が加えられていれば、記憶されている盗用元長検査値に該当する変更が行われない限り、そのオーバーレイファイルは無効になる。つぎに、不正変更防止オーバーレイの内容全体が、盗用元長検査値の位置が不明になるような方法で暗号化されるので、この値の存在をつきとめてそれを変更することが困難になる。

また、暗号化により、不正変更防止オーバーレイに含まれる特定のプログラム命令ならびに独自の盗用者識別および使用許諾制御データははっきりしなくなる。暗号化は、公開暗号化システムのように暗号化と復号に別々のキーを使用する技術によって達成される。暗号化ならびに独自の暗号化キーおよび解読キー発生のためのアルゴリズムは盗用システム内に格納し、したがって盗用者にはアクセスが不可能である。解読キーは、登録システムと登録プログラムシミュラを通じて盗用者のコンピュータに転送される。オーバーレイファイルを解読するためのアルゴリズムはローダーセグメント内にあるので、解読キーと解読アルゴリズムを使用してオーバーレイファイルを解読しその内容を検査することは、困難ではあるが可能である。しかし、内容を監視して、新しい変更されたオーバーレイファイルを暗号化する試みは、暗号化キーに対するアクセスができないために阻止される。私的暗号化キーで暗号化されたオーバーレイファイルだけしか盗用者識別データで解読できず、私的キーは盗用者から秘密には保たれないというのが、公開暗号化システムの特徴である。

不正変更防止オーバーレイファイルは、プログラム命令のエグゼクティブ制御ルーブセグメントと、使用許諾の方法と制御に適切な独自の盗用者識別データを含有している。このデータには、

盗用者識別の期間、コンピュータの製造番号、コンピュータのモデムの電話番号、そしてその他の情報が含まれる。

ローダーセグメント18は盗用目的のサブプログラムであり、これは、ローダープログラムが取り除かれたり盗用された場合、メインプログラムファイルを動作不能にする方法によって製品応用プログラムのメインプログラムファイルに結合される。この結合方法は、特定のプログラム命令と製品応用プログラムのメインプログラムファイル内部に内蔵するプロセスである。これらの内蔵された命令は、使用者にとっては未知の記憶位置にある特定の値を検査する。ローダープログラムセグメントを実行すると、特定の値がメインプログラムファイルの動作を可能にするのに必要な特定の記憶アドレス位置に記憶される。ローダープログラムセグメントは、その他の適性の知にこの動作を実行する。したがって、ローダーセグメントを取り外したり戻したりすると、メインプログラムファイルには特定の位置における特定の値が含まれないことになり、そのため動作不能になる。

図の実施例において、登録シェルは、製品応用プログラムの動作可能なデモンストレーション版を含んでいる可能性があるマーケティングパッケージの一部として配布される。デモンストレーション版のプログラムは、ローダーセグメント、デモンストレーション版の解読キー、そしてデモンストレーション版の不正変更防止オーバーレイを含むように設計されている。この場合、不正変更防止オーバーレイには独自の盗用者データは含まれないが、登録版の製品の価格と表示のデモンストレーションだけを行なうメインプログラムエグゼクティブ制御ルーブが含まれるであろう。デモンストレーション版のエグゼクティブ制御ルーブは、エグゼクティブ制御ルーブの簡易設計によって提供されたプログラムの盗用を許容している。たとえば、盗用版を提供するデモンストレーションシミュラをプログラミングして盗用版を表示することが出来るが、デモンストレーション版のエグゼクティブ

制御ルーブをプログラミングして盗用項目を製品登録依頼として解釈して、製品を動作させる前に登録することを要求できる。

登録を開始する前に、見込み盗用者はプログラムを実行し、デモンストレーション版が実行されておらず、固定しそして図3に示したように、デモンストレーション版の解読キーが使用され、デモンストレーション版のエグゼクティブ制御ルーブがロード、解読、そして実行される。デモンストレーションキーが終了すると、見込み盗用者は、使用書として登録し登録版のプログラムを実行するための一時的な使用許諾を得るようになる。そして、使用者は前述のようにして登録を行い、図4に示されているプロセスを開始することができる。登録要求に答えて、新しいオーバーレイファイル40と独自の解読キー20が含まれている盗用ファイルが盗用コンピュータから送られる。盗用プログラムファイルと更新版のプログラムファイルも、盗用ファイルと共に受信される。登録プログラムはデモンストレーション版の不正変更防止オーバーレイ40と解読キー20をそれぞれの登録版40と20で置き換える。

登録に続く、使用者がプログラムを実行すると、プログラム実行過程で登録版の不正変更防止オーバーレイ40が検出されてロードされ、独自の解読キー20を使用することにより、登録版のエグゼクティブ制御ルーブが解読され実行される。このようにして、デモンストレーション版は完全に動作する登録版に交換される。

プログラムの機向上版が利用出来る場合、使用者は同一のプロセスを移動してさらに別の解読キーと、より強化されたエグゼクティブ制御ルーブと追加プログラムファイルを含む別の不正変更防止オーバーレイとを受信して、より強化された版の製品に更新することが出来る。

様々な実施例が、小さな不正変更防止オーバーレイを使用して大きなプログラムの制御を行なうための適切で簡便な方法を提

表 6-501120 (7)

用することができる。このような状況は、ここにも含まれているように、プログラムの部分あるいはプログラム全体を使用許諾契約と併せる形式で配布するための、ここに開示されている方法がもたらす商業的利益の可能性の早なる例である。

上記の知見に照らし合わせ、本発明は様々な実施例が可能なのは明らかである。たとえば、本発明は、使用者のコンピュータがその地域の登録用コンピュータに接続され、あるいはその登録用コンピュータがそれより広い地域の登録用コンピュータに接続され、というように地理的に実装することも可能である。その地域の登録用コンピュータの登録範囲は、その地域の登録用コンピュータとそれより広い地域の登録用コンピュータとの契約に含まれる使用許諾制御データによって制御できるであろう。したがって、下記の特許請求の範囲内であれば、本発明を上記明細書に説明されている以外の方で実施することができる。

図 1

登録過程

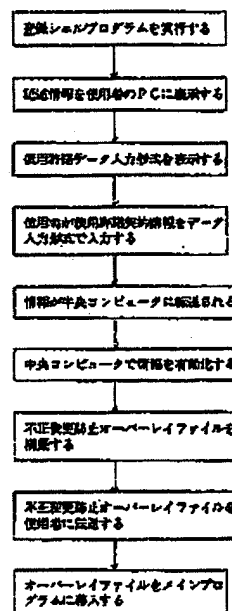
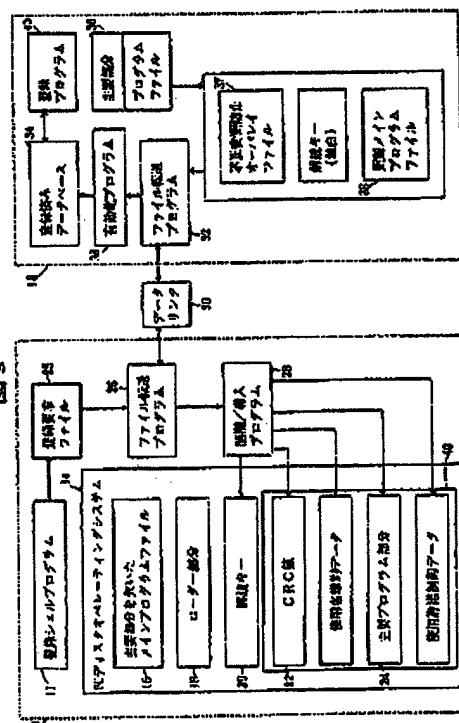
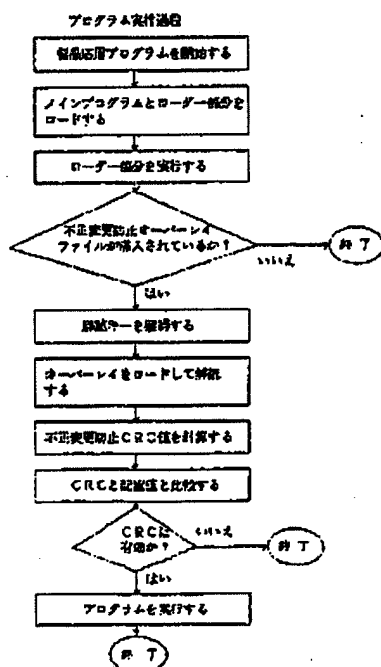
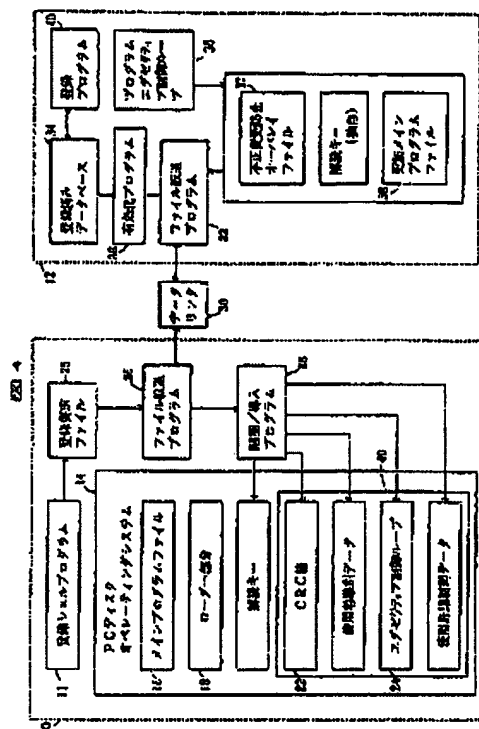


図 2



[illegible]

(S1) Int. Cl. 5

識別記号 庁内整理番号

F 1

HQ 4 L 9/12

(61)指定国 EP(AT, BE, CH, DE, DK, ES, FR, GB, GR, IT, LU, NL, S E), CA, JP